KISTI Certification Authority
Certificate Policy and Certification Practice Statement

Version 3.0 (March 20, 2017)

Korea Institute of Science and Technology Information (KISTI), Republic of Korea

Contents

1. Introduction

1.1. Overview

- Korea Institute of Science and Technology Information (KISTI) is a government-funded research institute located in Daejeon, Republic of Korea.
- This document is structured according to the RFC3647
- Not all sections of RFC3647 are used. Sections that are not included have a default value of "No stipulation."
- This document describes the set of rules and procedures established by the Korea Institute of Science and Technology Information Certification Authority (KISTI CA) for the operations of the KISTI PKI service.
- This document will include both the Certificate Policy and the Certificate Practice Statement for the KISTI PKI which is a traditional X.509 Public Key Certificate Authority that complies with the "Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure (OID: 1.2.840.113612.5.2.2.1.5.0)"* of IGTF.
  * https://www.eugridpma.org/guidelines/classic
- Intent of the KISTI CA PKI is to issue identity and service certificates for use in grid.

1.2. Document Name and Identification

- Document title:
  KISTI CA Certificate Policy and Certification Practice Statement
- Document version: **3.0**
- Document date: **February 17, 2017**
- OID:
  The following ASN.1 Object Identifier (OID) has been assigned to this document:
  1.3.6.1.4.1.14305.1.2.1.3.0
  This OID is constructed as shown in the table below:

IANA	1.3.6.1.4.1
KISTI(Korea Institute of Science and Technology Information)	14305
KISTI Supercomputing Center	1
KISTI CA	2
CP/CPS	1
Major Version	3
Minor Version	0

1.3. PKI Participants

1.3.1. Certification Authority

The KISTI CA does not issue certificates to subordinate certification authorities.

1.3.2. Registration Authorities

The KISTI CA delegates the authentication of individual identity to Registration Authorities (RA). RAs must sign an agreement with the KISTI CA, stating their adherence to the procedures described in this document. RAs are not allowed to issue certificates under this CP/CPS. The following is the KISTI RA registration procedure:

- RA candidate must accept the CP/CPS and agree to all RA responsibilities.
- RA candidate must be an employee of the institution or organization and provide work ID or proof of work.
- Complete the RA application form and fax it to KISTI CA.
- Send a verification e-mail to KISTI CA.
- KISTI CA will then arrange face-to-face or online-video meeting with the RA candidate.
- After completing the request, KISTI CA will publish the RA contact information on KISTI CA website.

1.3.3. Subscribers (End Entities)

The KISTI PKI issues person, host and service certificates to members of KISTI and other individuals working on

- International or domestic research projects/programs involved in WLCG Project or grid infrastructure related projects
  - Grid projects in collaboration with KISTI
  - Programs involved in KISTI supercomputing research

The term end entity is used to refer to the holder of the private key. For a person certificate it will be the subscriber, but for a host or service certificate the end entity may be some process running on a machine.

The subscriber is required to:
- read and adhere to the procedures published in this document.
- generate a key pair using a trustworthy method.
- take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate, including:

- For user certificates
  - selecting a pass phrase of at minimum 12 characters
  - protecting the pass phrase from others
  - always using the pass phrase to encrypt the stored private key
  - never sharing the private key with other users
- For host/service certificates
  - storing them encrypted whenever possible
  - provide correct information and authorize the publication of the certificate.
  - use the certificates for the permitted uses only.

1.3.4 Relying parties

KISTI CA's relying parties includes the following:
- Employees of KISTI or research institutes in Korea
- Employees of international research institutes which collaborate with KISTI
- Collaborating organizations with KISTI Supercomputing Center

Relying parties' obligations are as follows:
- Must read the procedures published by the KISTI CA.
- Must use the certificates for the permitted uses only.
- Must notify KISTI CA of any security incidents. (Notification shall occur within the first 12 hours of initial knowledge of incident.)
- May verify that the certificate is not on the CRL before validating a certificate.

1.3.5 Other participants

No stipulation.

1.4. Certificate Usage

1.4.1. Appropriate certificate uses

Certificates from KISTI CA may be used in applications for the following purposes:

- Grid middleware

Certificates may also be used to satisfy other general or specific requirements of Grid computing.

1.4.2. Prohibited certificate uses

No other usage than described in section 1.4.1 is prohibited.

1.5. Policy Administration

1.5.1. Organization administering the document

KISTI CA is managed by Global Science experimental Data hub Center, KISTI.

1.5.2. Contact person

For inquiries regarding this document or the KISTI PKI service in general, please contact:

Sang Un Ahn
Global Science experimental Data hub Center, KISTI
245 Daehak-ro Yuseong-gu, 34141, Korea
Phone: +82-42-869-0840
Fax: +82-42-869-1068
Email: sahn@kisti.re.kr

Ilyeon Yeo
Global Science experimental Data hub Center, KISTI
245 Daehak-ro Yuseong-gu, 34141, Korea
Phone: +82-42-869-0658
Fax: +82-42-869-1068
Email: ilyeon9@kisti.re.kr

A mailing list containing KISTI CA managers has been setup to ensure quick response:
kisti-grid-ca@kisti.re.kr

1.5.3. Person determining CPS suitability for the policy

See section 1.5.2.

1.5.4. CPS approval procedures

The KISTI CA is responsible for the CP and CPS.
For the global grid collaboration, KISTI CA is a member of APGrid PMA and IGTF.
Major changes must be approved by the APGrid PMA community.
Minor changes can be done by KISTI CA staff, and should be notified through the APGrid PMA mailing list.

1.6. Definitions and Acronyms

Certification authority (CA)
An authority trusted by one or more users to create and assign public key certificates. Optionally the CA may create the user's keys. The CA is responsible for the public key certificates during their whole lifetime, not just for issuing them.

CA certificate
A certificate for one CA's public key issued by another CA.

Certificate policy (CP)
A named set of rules that indicates the applicability of a certificate to a particular community or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

Certification path
An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certification practice statement (CPS)
A statement of the practices that a certification authority employs in issuing certificates.

Certificate revocation list (CRL)
A time stamped list identifying revoked certificates, which is signed by a CA and made freely available in a public repository.

Issuing certification authority (issuing CA)
The CA that issues the certificate (see also Subject certification authority).

Public key certificate (PKC)
A data structure containing the public key of an end entity and some other information, which is digitally signed with the private key of the CA that issued it.

Public Key Infrastructure (PKI)
The set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke PKCs based on public key cryptography.

Registration authority (RA)

An entity that is responsible for identification and authentication of certificate subjects but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA). The term Local Registration Authority (LRA) is used elsewhere for the same concept.

Relying party

A recipient of a certificate who acts in reliance on that certificate or on digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

Subject certification authority (subject CA)

In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate.

2. Publication and Repository Responsibilities

2.1. Repositories

- The KISTI CA online repository is available at http://ca.gridcenter.or.kr/

2.2. Publication of certification information

KISTI CA publishes the following information through its online repository (web site http://ca.gridcenter.or.kr/).

- KISTI CA's root certificate
- End entity certificates issued by the KISTI CA
- CRLs (Certificate Revocation List) issued by KISTI CA
- KISTI CA's signing policy
- A copy of this Policy (CP/CPS)
- All the CP/CPS under which valid certificates are issued
- Other information relevant to the KISTI PKI

2.3. Time or frequency of publication

- Certificates must be published as soon as issued.
- CRLs will be published as soon as issued or refreshed on scheduled update
- All KISTI PKI documents will be published to the online repository as they are updated.

2.4. Access controls on repositories

- The online repository is available on a substantially 24/7 basis, subject to reasonable scheduled maintenance.
- The KISTI CA does not impose any access control on the information described in section 2.2

3. Identification and Authentication

3.1. Naming

3.1.1. Types of names

Identification of certificates will be according to X.500 distinguished name. (RFC2459)
The DN must be in the form of a X.501 printable string and must not be blank.

The following table shows attribute values for name.
Both the Organization Name 2 and Common Name are decided based on the data provided by subscribers when requesting certificates.

attributes	meaning	value
countryName	Country name	KR
organizationName	Organization Name 1	KISTI
organizationName	Organization Name 2	Based on application information
commonName	User name(client certificate)	
	Host name(host certificate)	

3.1.2. Need for names to be meaningful

The Subject Name in a certificate MUST have a reasonable association with the End Entity.
Each host certificate must be linked to a single network entity.
The common name of the host certificate must be the FQDN of the host.

3.1.3. Anonymity or pseudonymity of subscribers

The subscribers cannot be anonymous or pseudonymous.

3.1.4. Rules for interpreting various name forms

See section 3.1.1.

3.1.5. Uniqueness of names

- The Distinguished Name (DN) must be assigned unique among certificates issued by the KISTI CA.
- For user certificates each CN component will include the full name of the subscriber. The registration interface appends 8 random alphanumeric characters in front of the name (i.e. "12345678 Gil-Dong Hong") when constructing the common name for uniqueness.

- During the subscriber registration process, KISTI CA assigns an inherent 8-digit number to each subscriber. In the online request web site, the registration interface refers the inherent 8-digit number associated with the subscriber.
- When a subscriber re-keys his/her certificate, KISTI CA will not assign a new 8-digit number but use the same 8-digit number by inheriting subscriber's attribute to guarantee to issue a new certificate with the same DN.

3.1.6. Recognition, authentication, and role of trademarks

No Stipulation

3.2. Initial Identity Validation

3.2.1. Method to prove possession of private key

KISTI CA confirms the possession of a private key by verification of the CSR signature.

3.2.2. Authentication of organization identity

KISTI CA verifies the identity of organizations by checking that the organization is known to be part of KISTI or its related collaboration projects.

3.2.3. Authentication of individual identity

- User: A person who requests a user certificate will be identified by in person interview with the RA. A photo ID card with a photo image on it must be presented at the interview.
- Host or Service certificate: Requests must be authorized as a legal subscriber of the CA and RA's approval is required before issuing host/service certificates for a proof of the subscriber's title of the host/service FQDN.

3.2.4. Non-verified subscriber information

No Stipulation

3.2.5. Validation of authority

No Stipulation

3.2.6. Criteria for interoperation

No Stipulation

3.3. Identification and Authentication for Re-key Requests

3.3.1. Identification and authentication for routine re-key

This is covered by section 4.7.2.

3.3.2. Identification and authentication for re-key after revocation

Rekey after revocation follows the same rules as an initial registration.

3.4. Identification and Authentication for Revocation Requests

Contact the KISTI CA or an authorized RA using signed e-mail or telephone in order to verify his/her identity and the validity of the request.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

Enrollment Process is as follows:

- A user who requests a user certificate must have a face-to-face meeting with the RA and present a user application form to the RA. (The application form is available from the KISTI CA web site).
- The RA examines the request according to section 3.2.
- Once the user is identified, the RA will give a PIN (Personal Identification Number) to him/her, having him/her write down the PIN on the application form, and finally put the RA's signature on the user application form. (The PIN is to be used later on as a passphrase of WACC, which is required for online certificate request)
- The user will fax the application form to the CA.
- Upon receipt of the application form, the CA will have a contact with the RA who signed the application form, making sure that the RA has really signed it. The CA can contact the RA via signed e-mail or telephone.
- If the application form is approved, the KISTI CA will inform the user of the fact that the application form has been approved by sending him a web-access client certificate (WACC) which gives him/her an authority to access the online certificate request web site.
- Using the PIN given by the RA as a passphrase, the user will be able to import the WACC in his/her web browser.

Certificate application process is as follows:

- Once the WACC properly is imported into his/her web browser, the user is able to access the online certificate request web site to make certificate request by an online procedure.
- For the online procedure, the user should do the following:
  - Visit the KISTI online certificate request web site.
  - Upload a CSR (certificate signing request) which contains the public key that is to be generated by the user.
  - Send the CA an e-mail to let the CA know that he/she has uploaded a CSR
  - Wait for the certificate issuance
- Subscribers can generate a CSR for user certificate using following means:
  - Using OpenSSL or equivalent software

    - Using CSR generation service provided by KISTI CA in the certificate request web site
- Host/service certificate request is the same as the user certificate request case. To request a host/service certificate request, the subscriber must access the online certificate request web site of KISTI CA, which requires an enrollment process if the subscriber have no WACC. But, for the certificate application process of host/service certificates, RA's approval is required before issuing host/service certificates for a proof of the subscriber's title of the host/service FQDN. Subscriber should send the CA a signed e-mail to inform that a CSR has been uploaded.

4.2. Certificate Application Processing

4.2.1. Performing identification and authentication functions

KISTI CA ensures that the followings in the enrollment process and certificate application process:

In the enrollment process, the CA checks if
- the application form is correct; and
- the PIN number in the application form is correspond with the RA's generated number in the previous section; and
- the RA examined the subscriber in a face-to-face meeting or an equivalent inspection process, if required.

In the certificate application process, the CA checks if
- the certificate request is done in accordance with the process in this document especially in the section 4.1.
- the certificate request subject name has correct format; and
- the key length of the certificate request meets the requirement.

4.2.2. Approval or rejection of certificate applications

- The issuance of a certificate by the CA indicates a complete and final approval of the certificate application by the CA.
- If any condition specified in section 4.2.1 is not be satisfied, the certificate application is rejected and the CA notifies to the subscriber with the reason of the rejection.

4.2.3. Time to process certificate applications

- The CA should process the certificate application within 2 business day from the acceptance of the certificate request.

4.3. Certificate Issuance

- Upon the receipt of CSR, KISTI CA operator will store the CSR in a memory stick and take it to the KISTI signing machine which is kept off-line as described in section 6.7,
- The CA operator generates (issues) user certificate containing user public key with CA signature and hand-carrying it to the online public web server.
- A notification message is sent to the e-mail address of the subject with the instructions on how to download it from the online public web server.
- The user will be able to download his/her user certificate. For this secure HTTP connection is required.
- If the authentication is unsuccessful, the certificate is not issued and an e-mail with the reason is sent to the subject.

4.4. Certificate Acceptance

- If the issued certificate has any problem, the subscriber should notify the CA that he cannot accept the issued certificate with a proper reason within 7 days from issuance of the certificate.
- Unaccepted certificate should be revoked and the certificate should be re-issued.

4.5. Key Pair and Certificate Usage

- KISTI certificates may be used for any software for grid computing.
- They could be used in other capacities, but the KISTI CA does not recommend or warrant any other use of the certificates it signs.
- User certificates must not be shared between multiple people.
- Host certificates must be linked to a single network entity.
- The subscriber must manage his certificates and private keys securely. To protect the private key the subscriber must encrypt his private with a pass phrase. The pass phrase should be more than 12 characters long.

4.6. Certificate Renewal

4.6.1. Circumstance for certificate renewal

- Certificate renewal means the issuance of a new certificate to the subscriber without changing information in the certificate before expiration of the certificate. There are two possible cases:

- Renew a certificate with the same key:
  - KISTI CA does not permit certificate signing request with the same key as the previous certificate.
- Renew a certificate with a new key.
  - This case is regarded as certificate re-key, which is covered in section 4.7.

4.6.2. Who may request renewal

- Covered in section 4.7.2.

4.6.3. Processing certificate renewal requests

- Covered in section 4.7.3.

4.6.4. Notification of new certificate issuance to subscriber

- Covered in section 4.7.

4.6.5. Conduct constituting acceptance of a renewal certificate

- Covered in section 4.7.

4.6.6. Publication of the renewal certificate by the CA

- Covered in section 4.7.

4.6.7. Notification of certificate issuance by the CA to other entities

- Covered in section 4.7.

4.7. Certificate Re-key

4.7.1. Circumstance for certificate re-key

Generally, certificate re-key can or must take place in cases such as:
(Case 1) after a certificate is revoked for reasons of key compromise; or
(Case 2) after a certificate has expired and the usage period of the key pair has also expired; or
(Case 3) one (1) month prior to the expiration of the EE certificate.

4.7.2. Who may request certification of a new public key

- A subscriber of KISTI CA can request certification of a new public key in the following conditions.

- If a certificate of the subscriber is revoked for reasons of key compromise (case 1 in section 4.7.1).
- If a certificate has expired and the usage period of the key pair has also expired (case 2 in section 4.7.1).
- If a certificate is going to be expired in one month (case 3 in section 4.7.1).

4.7.3. Processing certificate re-keying requests

- If a certificate is revoked for reasons of key compromise (case 1 in section 4.7.1):
  - The compromised certificate must be revoked and the subscriber of the certificate should follow the enrollment process (of section 4.1) again to get a new certificate.
- If a certificate has expired and the usage period of the key pair has also expired (case 2 in section 4.7.1):

    - If the point of time of the re-key request has passed 3 years from the previous enrollment process of the subscriber, the subscriber is required follows a new enrollment process again.
- If a certificate expires in one (1) month (case 3 in section 4.7.1):
    - The subscriber can request a new certificate using the online certificate request web site mentioned in section 4.1. The subscriber must generate a new key pair for a new certificate and should upload the certificate signing request (CSR) in the online request web site. CSR generation method and its processing are the same as the initial certificate request in section 4.1.
    - If the point of time of the re-key request has passed 3 years from the previous enrollment process of the subscriber, the subscriber is required follows a new enrollment process again.
    - If a subscriber apply to renew his/her EE certificate prior to the expiration of the EE certificate, CA operator should revoke the previous EE certificate within 1 week after issuing the new certificate but not after the expiration time of the old certificate.
    - KISTI CA does not permit certificate signing request with the same key as the previous certificate. The new certificate request must use a different key with the previous certificate.

4.7.4. Notification of new certificate issuance to subscriber

- Basically same as the initial certificate issuance in the section 4.1.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

- Basically same as the initial certificate issuance in the section 4.1.

4.7.6. Publication of the re-keyed certificate by the CA

- Basically same as the initial certificate issuance in the section 4.1.

4.7.7. Notification of certificate issuance by the CA to other entities

- Basically same as the initial certificate issuance in the section 4.1.

4.8. Certificate Modification

KISTI CA does not support certificate modification.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for revocation

A certificate must be revoked when information it contains is suspected to be incorrect or compromised. This includes situations where:

- The subscriber's private key is compromised or is suspected to have been compromised.
- The subscriber's information in the certificate is suspected to be inaccurate.
- The subscriber is known to have violated his obligations which could induce a critical security hole.
- The subscriber leaves his/her organization.
- In case of host/service certificates, the corresponding host/service is retired.

4.9.2. Who Can Request Revocation

KISTI CA will accept a revocation request made by

- The certificate subscriber
- KISTI CA/RA
- Any other entity presenting evidence of circumstances as described in section 4.9.1.

4.9.3. Procedure for Revocation Request

Entities requesting revocation of a certificate must authenticate themselves in one of the following ways:

- Sending an email, maybe signed by a valid and trusted certificate, to kisti-grid-ca@kisti.re.kr, RA will contact the subscriber for confirmation via e-mail or telephone.
- In the other cases, authentication is performed with the same procedure used to authenticate the identity of person.

In both case above, the requesting entity must specify the reason for the revocation request and provide evidence of circumstances as described in section 4.9.1.

4.9.4. Revocation request grace period

- CA will process revocation as soon as it receives the revocation request and the request is approved.
- The revocation information will be published to the online repository.
- During the revocation, a revocation notification is sent to the subscriber through the subscriber's email.

4.9.5. Time within which CA must process the revocation request

The CA should process the certificate revocation request within 1 working day from the recognition of the request.

4.9.6. Revocation checking requirement for relying parties

No stipulation.

4.9.7. CRL Issuance Frequency (if applicable)

- The lifetime of the CRL is 30 days.

- A new CRL is issued immediately after a revocation or at least 7 days before expiration.

4.9.8. Maximum latency for CRLs (if applicable)

- CRLs must be published in the repository after generation as soon as possible.
- In KISTI CA, the maximum latency between the generation of CRLs and posting of the CRLs to the repository is 1 hour.

4.9.9. On-line revocation/status checking availability

KISTI PKI system does not provide any online status checking facility.

4.9.10. On-line revocation checking requirements

KISTI PKI system does not provide any online status checking facility.

4.9.11. Other forms of revocation advertisements available

No stipulation.

4.9.12. Special requirements re key compromise

No stipulation.

4.9.13. Circumstances for suspension

KISTI CA does not support Certificate Suspension.

4.9.14. Who can request suspension

KISTI CA does not support Certificate Suspension.

4.9.15. Procedure for suspension request

KISTI CA does not support Certificate Suspension.

4.9.16. Limits on suspension period

KISTI CA does not support Certificate Suspension.

4.10. Certificate Status Services

KISTI CA does not support (on-line) certificate status services.

4.11. End of Subscription

If a subscriber of KISTI CA end the subscription to the CA services:

The subscriber must do the following:
- Must not use any certificate issued from KISTI CA
- Must delete his WACC (from section 4.1) from his web browser.

The CA must do the following:
- Must revoked all certificates issued for the subscriber.
- Must disable any authentication for the user's WACC

4.12. Key Escrow and Recovery

No stipulation.

5. Management, Operational, and Physical Controls

5.1. Physical Security Controls

The CA operates in a controlled environment, where access is restricted to authorized people.

5.1.1. Site location and construction

KISTI PKI is located at Global Science experimental Data hub Center, KISTI at Daejeon, Korea.

5.1.2. Physical access

Physical access to the KISTI CA machine is restricted to authorized personnel.
The KISTI CA machines (both the issuing machine and the public web server) are:

- running on dedicated machines.
- located in a secure environment where access is controlled.
- professionally managed.

5.1.3. Power and air conditioning

The CA signing machine and the CA web server are both protected by uninterruptible power supplies. Environment temperature in rooms containing CA related equipment is maintained at appropriate levels by suitable air conditioning systems.

5.1.4. Water exposures

The CA shall ensure that the CA system is adequately protected from water exposures.

5.1.5. Fire prevention and protection

The building housing the KISTI CA facilities has a fire alarm system.
The CA shall ensure that the CA system is adequately protected from fire by a fire suppression system.

5.1.6. Media storage

The KISTI CA key and backup copies of CA related information is securely kept in several removable storage media.

5.1.7. Waste disposal

The CA shall ensure that all media containing sensitive information is sanitized, to remove information such that data recovery is not possible, or destroyed before release for disposal. CA personnel shall account for the destruction of sensitive information.

5.1.8. Off-site backup

In KISTI CA, No off-site backups are currently performed.

5.2. Procedural Controls

5.2.1. Trusted roles

- SYSTEM ADMINISTRATOR (SYSADM) has full control over the CA server and software.
- CERTIFICATE AUTHORITY OPERATOR (CAO) can manage all certificates, requests and cryptographic data including CA private key. CAO is contact point for subscribers about CA operation. CAO can make changes of CP/CPS.
- REGISTRATION AUTHORITY OPERATOR (RAO) examines subscriber's information and checks the trust of the subscriber in behalf of certificate authority.
- SYSTEM AUDITOR (SA) has read-only access to all components of the PKI system to verify the operation complies with the rules and regulations of this CP/CPS. SA approves any changes of CP/CPS by CAO in prior to an approval of the regional PMA (APGrid PMA).

5.2.2. Number of persons required per task

For operation of KISTI PKI, the number of persons required for the roles is:

- SYSTEM ADMINISTRATOR: 1 person or more.
- CERTIFICATE AUTHORITY OPERATOR: 2 persons or more for back-up each other.
- REGISTRATION AUTHORITY OPERATOR: 1 person or more for each RA site.
- SYSTEM AUDITOR: 1 person or more.

5.2.3. Identification and authentication for each role

In KISTI PKI, on-line and/or off-line system will identify and authenticate the operator when the staff operates the system.

5.2.4. Roles requiring separation of duties

- SYSTEM AUDITOR may not be a SYSTEM ADMINISTRATOR, or CERTIFICATE AUTHORITY OPERATOR.

5.3. Personnel Security Controls

All access to the servers and applications that comprise the KISTI PKI is limited to KISTI PKI security staffs.

5.3.1. Qualifications, experience, and clearance requirements

The CA shall ensure that all staff performing CA and RA functions possesses the necessary knowledge, experience and qualifications to perform their duties.

5.3.2. Background check procedures

CA personnel must be a formal member of KISTI.

5.3.3. Training requirements

Internal training is given to KISTI CA and RA operators.

5.3.4. Retraining frequency and requirements

No Stipulation

5.3.5. Job rotation frequency and sequence

No stipulation.

5.3.6. Sanctions for unauthorized actions

In the event of actual or suspected unauthorized actions by a person performing duties with respect to the operation of the CA or an RA, the CA shall suspend his or her access to the CA system.

5.3.7. Independent contractor requirements

The CA shall ensure that contract personnel satisfy the same personnel security requirements with respect to appointment, training and background checks as those applicable to CA employees.

5.3.8. Documentation supplied to personnel

The CA shall provide these Certificate Policies, relevant provisions of the CPS, as well as any specific statutes, policies or contracts relevant to their positions to CA personnel, RAs and Client Responsible Individuals.

5.4. Audit Logging Procedures

- The KISTI CA will retain records as much as possible so that the KISTI CA could trace anything if something illegal would happen.
- Such audit information is not publicly available.
- Auditors are allowed to access the information as part of auditing and such information must be kept confidential.
- CA operator performs operational audits of the CA/RA staff at least once per year.

5.4.1. Types of events recorded

- Certification requests
- Revocation requests
- Issued certificates
- Issued CRLs
- Logs of commands such as shutdown/boot/reboot/login/logout/sudo on the CA machine and on-line request web server.
- Other logs archived by UNIX operating of the CA machine and RA server

5.4.2. Frequency of processing log

The CA shall ensure that all significant events are explained in an audit log summary and that CA personnel review audit logs at least once every month. Such reviews involve verifying that the log has not been tampered with, and then inspecting all log entries. CA personnel shall conduct a more thorough investigation of any "alerts" or irregularities in the logs. The CA shall indicate who has responsibility for audit log review and audit log summary preparation in the CPS.

5.4.3. Retention period for audit log

The CA shall retain its audit logs on site for at least two (2) months and subsequently retain audit logs in the manner described in section 5.5.

5.4.4. Protection of audit log

The CA shall protect the electronic audit log system and audit information captured electronically or manually from unauthorized viewing, modification, deletion or destruction.

5.4.5. Audit log backup procedures

The CA shall back up or copy all audit logs and audit summaries.

5.4.6. Audit collection system (internal vs. external)

No stipulation.

5.4.7. Notification to event-causing subject

No stipulation.

5.4.8. Vulnerability assessments

No stipulation.

5.5. Records Archival

5.5.1. Types of records archived

- CA's records archival
  - CA records all the types of events listed in section 5.4.1 are archived.
  - In addition to that, email sent to/from kisti-grid-ca@kisti.re.kr messages will be archived as well.
  - CA private keys must be backed up and protected at a level of physical and cryptographic protection equal to or exceeding that in place at the CA site.
- RA's records archival
  - RA records all the types of events regarding user registration, certificate/revocation request including:
    - date of meeting with a subscriber
    - evidence of identity of a subscriber
    - email messages sent to/from the RA's email address.

5.5.2. Retention period for archive

Certificates and CRLs generated by the CA, must be retained for at least 2 years after their expiration, and;
The minimum retention period is 3 years.

5.5.3. Protection of archive

System logs and email archives are protected by the authorization mechanism provided by UNIX operating system. Only the owners of the system logs are able to modify the logs. System logs and email archives are periodically back-up to the offline media which is stored in a safe place.

5.5.4. Archive backup procedures

A second copy of all material retained or backed up must be stored in read-only media like CD-ROM.
The second copy must be protected either by physical security alone, or a combination of physical and cryptographic protection.

5.5.5. Requirements for time-stamping of records

All archived logs and documents are time stamped.

5.5.6. Archive collection system (internal or external)

No stipulation.

5.5.7. Procedures to obtain and verify archive information

No stipulation.

5.6. Key Changeover

- When the CA's cryptographic data needs to be changed (e.g. CA key expiration), from the time of distribution of new cryptographic data, only the new CA certificate will be used for certificate signing purposes.
- From that time, the old CA certificate will not be used for certificate signing purposes.
- The overlap of the old and new CA certificate must be at least the longest time an end-entity certificate can be valid (1 year).
- The old CA certificate will be valid and available to verify old signatures and the secret key to sign CRLs until all the certificates signed using the associated private key have also expired.

5.7. Compromise and Disaster Recovery

- If it is detected that hardware, software or data are corrupted or damaged
  - Recover the system by using backup hardware, software, or data as quickly as possible.
- If a CA's private key is compromised or suspected to be compromised, the KISTI CA will:
  - Notify subscribers, RAs and relying parties.
  - Revoke all issued certificates.
  - Terminate the certificates and CRLs distribution service for certificates/CRLs issued using the compromised private key.
  - Create a new pair of key and re-build the CA system.

5.8. CA or RA Termination

Before KISTI CA terminates its services it will:

- Make publicly available information of its termination.
- Stop issuing certificates and CRLs.
- Destroy its private key's and all copies.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key pair generation

- A CA key pair is generated by CA staff on a signing machine which is not connected to any kind of network.
- End entities' cryptographic keys are locally generated by their application during the requesting process.
- KISTI PKI does not generate private keys for subjects.

6.1.2. Private key delivery to subscriber

The KISTI CA does not generate end entities' private keys hence does not deliver private keys. User's private key could be generated by browser application in personal computer.

6.1.3. Public key delivery to certificate issuer

End entity will send its public key included in CSR at time of certificate request.

6.1.4. CA public key delivery to relying parties

CA certificate will be published on the KISTI PKI repository.

6.1.5. Key sizes

- The minimum key length for user or host/service certificate is 2048 bits.
- The CA key length is 4096 bits.

6.1.6. Public key parameters generation and quality checking

No stipulation

6.1.7. Key usage purposes (as per X.509 v3 key usage field)

KISTI CA private key is the only key used for signing CRLs and Certificates for persons, servers and services. The Certificate key Usage field must be used in accordance with the “Internet X.509 Public Key Infrastructure Certificate and CRL profile” [RFC 2459].

6.2. Private Key Protection and Cryptographic Module Engineering

6.2.1. Cryptographic module standards and controls

KISTI CA does not use any hardware security module.

6.2.2. Private key (n out of m) multi person control

In KISTI CA system, (n out of m) multi-person control is not supported. The passphrase for accessing to CA's private key is known to 2 CA staffs.

6.2.3. Private key escrow

Not supported.

6.2.4. Private key backup

The KISTI private key backup is performed by CA operator and the two copies of backup key is kept encrypted in a CDROM and memory stick respectively in a safe place where access is controlled.

6.2.5. Private key archival

See section 5.5.

6.2.6. Private key transfer into or from a cryptographic module

No stipulation.

6.2.7. Private key storage on cryptographic module

No stipulation.

6.2.8. Method of activating private key

See section 6.4.

6.2.9. Method of deactivating private key

No stipulation.

6.2.10. Method of destroying private key

No stipulation.

6.2.11. Cryptographic Module Rating

No stipulation.

6.3. Other Aspects of Key Pair Management

6.3.1. Public key archival

The CA shall retain all public key certificates it generates.

6.3.2. Certificate operational periods and key pair usage periods

- The lifetime of KISTI CA certificate is twenty (20) years.
- The lifetime of user certificate is 400 days.
- The lifetime of host certificate is 400 days.

6.4. Activation Data

- The KISTI CA's private key is protected by a pass phrase over 15 characters.
- This pass phrase is only known by CA operators.
- The pass phrase is in a sealed envelope kept in a safe place where access is controlled.
- But the sealed envelope is kept separated from the backed private key.

6.5. Computer Security Controls

6.5.1. Specific computer security technical requirements

- CA operating systems are maintained at a high level of security by applying all the relevant patches.
- Monitoring is performed to detect unauthorized software changes.
- CA systems configuration is reduced to the base minimum.
- Both CA signing machine and web server machine are used for dedicated purpose respectively.

6.5.2. Computer security rating

No stipulation.

6.6. Life Cycle Security Controls

No stipulation.

6.7. Network Security Controls

- The CA signing machine is kept off-line.
- The CA web server machine is protected by a firewall.
- The CA web server machine is a dedicated machine and no network service other than CA web server run on the server.
- Appropriate software upgrade/patch of the CA web server is performed every 6 month or immediately if it is required.

6.8. Time-stamping

No stipulation.

7. Certificate and CRL Profiles

7.1. Certificate Profile

7.1.1. Version number(s)

X.509 v3.

7.1.2. Certificate extensions

CA Certificate:

- X509v3 Basic Constraints: critical, CA:TRUE
- X509v3 Key Usage: critical, Certificate Sign (keyCertSign), CRL Sign (cRLSign),
- Certificate Policies: 1.3.6.1.4.1.14305.1.2.1.3.0

User Certificates:

- X509v3 Basic Constraints: critical, CA:FALSE
- X509v3 Key Usage: critical, Digital Signature (digitalSignature), Non Repudiation (nonRepudiation), Key Encipherment (keyEncipherment), Data Encipherment (dataEncipherment)
- X509v3 Extended Key Usage: TLS Web Client Authentication (clientAuth)
- X509v3 Issuer Alternative Name: email: kisti-grid-ca@kisti.re.kr~~,~~ URI:http://ca.gridcenter.or.kr/
- X509v3 CRL Distribution Points: URI:http://ca.gridcenter.or.kr/CRL/
- Certificate Policies: 1.3.6.1.4.1.14305.1.2.1.3.0

Host Certificates:

- X509v3 Basic Constraints: critical, CA:FALSE
- X509v3 Key Usage: critical, Digital Signature (digitalSignature), Key Encipherment (keyEncipherment), Data Encipherment (dataEncipherment)
- X509v3 Extended Key Usage: TLS Web Server Authentication(serverAuth), TLS Web Client Authentication(clientAuth)
- X509v3 Issuer Alternative Name: email: kisti-grid-ca@kisti.re.kr, URI:http://ca.gridcenter.or.kr/
- X509v3 Subject Alternative Name: DNS:<FQDN of the host>
- X509v3 CRL Distribution Points: URI:http://ca.gridcenter.or.kr/CRL/
- Certificate Policies: 1.3.6.1.4.1.14305.1.2.1.3.0

X.509v3 Extension	**CA Certificate**	**User Certificates**	**Host Certificates**
Basic Constraints	critical, CA:TRUE	critical, CA:FALSE	critical, CA:FALSE
Key Usage	critical	critical	critical
Key Usage:Certificate Sign	O	-	-
Key Usage:CRL Sign	O	-	-
Key Usage:Digital Signature	O	O	O
Key Usage:Non Repudiation	O	O	-

Key Usage:Key Encipherment	O	O	O
Key Usage:Data Encipherment	-	O	O
Extended Key Usage	-	TLS Web Client Authentication(clientAuth)	TLS Web Server Authentication(serverAuth), TLS Web Client Authentication(clientAuth)
Issuer Alternative Name	-	email: kisti-grid-ca@kisti.re.kr, URI:http://ca.gridcenter.or.kr/	email: kisti-grid-ca@kisti.re.kr, URI:http://ca.gridcenter.or.kr/
Subject Alternative Name	-	-	DNS:<FQDN of the host>
CRL Distribution Points	-	URI:http://ca.gridcenter.or.kr/CRL/	URI:http://ca.gridcenter.or.kr/CRL/
Certificate Policies	1.3.6.1.4.1.14305.1.2.1.3.0	1.3.6.1.4.1.14305.1.2.1.3.0	1.3.6.1.4.1.14305.1.2.1.3.0

7.1.3. Algorithm object identifiers

Signature Algorithm: sha256WithRSAEncryption (2048 bits)

7.1.4. Name forms

- Issuer:
  C=KR, O=KISTI, CN=KISTI Certification Authority
- User DN:
  C=KR, O=KISTI, O=[applicant's organization], CN=[the name of applicant]
- Host DN:
  C=KR, O=KISTI, O=[applicant's organization], CN=[FQDN of the hostname]

7.1.5. Name constraints

Subject DN can contain the following characters:
Alphabetic characters: a-z, A-Z
Numerical character: 0-9
Special character: - (dash), _ (underscore)

No other characters are allowed for the subject name.

7.1.6 Certificate policy object identifier

X509v3 Certificate Policies: Policy: 1.3.6.1.4.1.14305.1.2.1.3.0
See section 1.2.

7.1.7 Usage of policy constraints extensions

No Stipulation.

7.1.8 Policy qualifier syntax and semantics

No Stipulation.

7.1.9. Processing semantics for the critical Certificate Policies extension

No Stipulation.

7.2. CRL Profile

CRLs are signed by the KISTI CA private key and are published in a web page.

7.2.1. Version number(s)

X.509 v2.

7.2.2. CRL and CRL entry extensions

Message digest algorithm of the CRL: SHA256

7.3. OCSP Profile

7.3.1. Version number(s)

No stipulation.

7.3.2. OCSP extensions

No stipulation.

8. Compliance Audit and Other Assessment

8.1. Frequency of Entity Compliance Assessment

The KISTI CA will accept external Compliance Audit. In addition, the KISTI CA performs operational self-assessment of CA/RA staff at least once per year.

8.2. Identity/Qualifications of Assessor

KISTI CA can be audited by the APGrid PMA.

8.3. Assessor's relationship to assessed entity

KISTI CA can be audited by the APGrid PMA.

8.4. Topics Covered by Assessment

Audit items will be selected based on the minimum CA requirements and documents enacted by the APGrid PMA.

8.5. Actions Taken as a Result of Deficiency

The KISTI CA has the responsibility for the action to be taken as a result of deficiency. When the KISTI CA receives an audit report from the auditor, it will send a report on actions to the auditor within two weeks. The report must describe actions taken as a result of deficiency and their timetable.

8.6. Communications of Results

The result of the audit will be made available to APGrid PMA in which the KISTI CA participates. It may make the results of the audit publicly available.

9. Other Business and Legal Matters

9.1. Fees

No fees are charged for any service provided by the KISTI CA.

9.2. Financial Responsibility

Accept no liability at all.

9.3. Confidentiality of Business Information

- KISTI CA collects subscriber's full names and email addresses. Some of this information is used to construct unique, meaningful subject names in the issued certificates.
- Information included in issued certificates and CRLs is not considered confidential.
- KISTI PKI does not collect any kind of confidential information.
- KISTI PKI does not have access to or generate the private keys of a digital signature key pair, such as those used in KISTI identity certificates. These key pairs are generated and managed by the subscribers and are the sole responsibility of the subscribers.

9.4. Privacy of Personal Information

The subscriber's private information collected for registration are:
- Name of subscriber
- Gender of subscriber
- Country
- Organization Name
- Position
- Telephone
- Email

We do not provide this information to other organizations.

9.5. Intellectual Property Rights

All certificate related data issued by KISTI CA is not under any copyright or intellectual property protection.

9.6. Representations and Warranties

No stipulation.

9.7. Disclaimers of Warranties

No stipulation.

9.8. Limitations of Liability

- KISTI PKI issues person certificates according to the practices described in this document.
- KISTI PKI makes no guarantee about the security or suitability of a service that is identified by a KISTI certificate.
- The certification service is run with a reasonable level of security, but it is provided on a best effort only basis.
- It does not warrant its procedures and it will take no responsibility for problems arising from its operation, or for the use made of the certificates it provides.
- KISTI PKI denies any financial or any other kind of responsibility for damages or impairments resulting from its operation.

9.9. Indemnities

No stipulation.

9.10. Term and Termination

9.10.1. Term

This CP/CPS is valid and enforceable from the time of accreditation by APGrid PMA.

9.10.2. Termination

This CP/CPS terminates in the following cases:
- CA certificate expires
- CA terminates its service
- A new version of CP/CPS is accredited.

9.10.3. Effect of termination and survival

No stipulation.

9.11. Individual notices and communications with participants

No stipulation.

9.12. Amendments

- Users will not be warned in advance of changes to the KISTI CA's policy and CPS.
- Any revision of specification is made by KISTI CA and it is approved by the APGrid PMA.
- New OID will be assigned to the revised document whenever there is a material change.
- Material changes should be approved by the APGrid PMA before signing any certificates under the new CP/CPS.

9.13. Dispute Resolution Procedures

No stipulation.

9.14. Governing Law

KISTI CA is subject to Korean law.

9.15. Compliance with Applicable Law

No stipulation.

9.16. Miscellaneous Provisions

No stipulation.

9.17. Other Provisions

No stipulation.